SECTION 281300 – ACCESS CONTROL SYSTEM FOR ELECTRONIC SECURITY

PART 1 - GENERAL

1.1 SUMMARY

A. Related Documents: Drawings and general provisions of contract, including general conditions and other Division 1 specification sections, apply to the work of this section.

B. Work of This Section:

1. This Section describes the components, configuration and operational sequences of the electronic access control and intrusion detection system including but not limited to the control and processing (head end) equipment, security workstations, operating systems/software, access control system panels, controllers, power supplies, electric strikes, electric hinges, door position switches, request to exit motion detectors, card readers, keypad/readers, card key switch overrides and systems interfaces.
2. Products furnished but not installed under this section:
3. Products installed but not furnished under this section:
   a. Lockset and Deadbolt cylinder cores: Furnished by Owner, installed by Contractor.

C. Related Requirements:

1. The Owner has access control and intrusion detection system standards that include proprietary products. Substitutions for proprietary equipment, components and products are not permitted.
2. Proprietary manufacturer for access control panels, software and controls: IDenticard PremiSys Control.
   a. Control panels shall communicate over TCP/IP to the existing Loudoun County IDentiPASS Plus SQL server.

1.2 SYSTEM DESCRIPTION

A. Access Control System

1. Furnish and install a complete and functional access control system. Provide coordination to ensure that the system furnished includes integration of, or interfacing to all devices and systems.
2. System will control locking devices for architectural, overhead, and detention style doors.
3. Provide programming that integrates control of devices indicated in the project documents.
4. Provide operating software on security systems PC allowing for user initiated changes to the system.
5. Access control system will interface with the alarm system. Valid card read will be used to shunt the alarm system allowing staff to enter the building during off hours. Request to exit switches integral to door hardware will be used to shunt the alarm system allowing staff to exit the building after hours.
6. Access control system will interface with handicap accessible doors. When the building is secured, a valid card read unlocks the door, then activates the paddle activating the door opener.
7. Access control system will interface with overhead doors for vehicle sallyport.

a. Valid card read at pedestal mounted card reader will open overhead door.
b. After the vehicle has entered the sally port the staff at Security will close the door.
c. A close only push button will be located adjacent each door allowing staff to close the each door.
d. When staff exit the sallyport the vehicle will pass over a loop detector located outside the sallyport. Once the vehicle passes over the loop the loop detector module will signal the overhead door operator to start the close sequence.
e. Contractor shall coordinate spacing, size, and location of vehicle detection loops in accordance with the manufacturer's recommendations.

8. The Access control system shall include a graphical user interface loaded on workstations (furnished by the County) as directed by the County. The contractor shall coordinate with the County the installation of the access control software on County furnished workstations. This user interface will be used for over-ride control of all controlled doors and alarm reporting. Scaled floor plans are required for visual indication of the status of all doors and alarm points in the building. Integral speakers will be required for audible indication of alarm points (provided by the County).
9. Provide Access Control operating software for user initiated modifications to the access control system.

10. Access control will provide for group and individual remote release function.
11. Provide Access Control operating software for user initiated modifications to the access control system.
12. Duress alarms will automatically call to local sheriff's office.
13. DPS switches are required on all doors notifying access control system of unsecure openings.

1.3 REFERENCES

A. Standards
1. UL 294 - Standard for Access Control System
2. Factory Mutual (FM) approval
3. Americans with Disabilities Act (ADA)
4. MC Directive 89/336/EEC
5. Electromagnetic Compatibility Requirements
6. Product Standard EN 55011: 1991Generic Standard EN 50082-2: 1995

1.4 ADMINISTRATIVE REQUIREMENTS

A. Coordination
1. Provide all junction boxes, conduits, 110VAC circuits at locations requiring 110VAC power supplies.
2. Provide one 6" x 6" x 6' trough in Room 129 for connecting conduits from field locations. The network connection RJ45 data jacks shall be provided at locations requiring data drops.
3. One analog telephone line shall be supplied in room 129 at security panel location. Provide one N/C fire alarm relay that changes state when fire alarm system is in alarm state and/or when there is a loss of power to the fire control panel in the IT/COM room.
4. Space in the network rack will be provided by the Owner in Room 129 and will be used to house the CCTV recording equipment provided under related sections.

1.5 SUBMITTALS

A. Informational Submittals:

1. Bill of Materials: Provide a complete list of materials and equipment proposed for use on this project, including quantities, manufacturer, model numbers and a brief description of each item.
2. Installers Certification: Prior to commencement of work submit an original signed document from the manufacturer's authorized representative, certifying that the Installer is fully trained and certified to design, document, furnish, install, program and test the installed equipment and systems.
3. Testing and Demostration Plans
    a. Provide a testing plan for all devices and systems, including minimal acceptable performance requirements, methods of testing, testing schedule, forms and instrumentation.
    b. Provide a systems demonstration plan, to provide verification that the configuration and system programming implements the approved sequences of operation and the Owner requirements.

B. Action Submittals

1. Product Data: Submit manufacturer's standard product data sheets for all equipment proposed.
    a. Product Data shall be submitted with the Bill of Materials submittal listed above.
    b. Product data shall include at a minimum a brief description of the product proposed, standard features, physical characteristics, dimensions, weight, mounting details, electrical specifications, connection requirements and sequence of operation.
    c. Product Data shall also include all Nationally Recognized Testing Laboratory (NRTL) listing data for the proposed product, both as an individual component and as part of a system.
2. Shop or Coordination Drawings/Delegated Design Submittals: Provide Installation/Coordination Documents including but not limited to specifications, manufacturer's installation instructions, and project specific drawings for the electronic access control and security system.
3. Where required by Authorities having Jurisdiction for trade permits, provide professional of record services by a professional engineer licensed in the Commonwealth of Virginia that is certified as a Registered Communication Distribution Designer (RCDD.) Installation/Coordination Drawings shall include;
    a. Symbols, legends, notes and general information sheet.
    b. Floor plans noting the locations of all security devices, door hardware devices, CCTV cameras, security equipment cabinets, security network panels, reader interface panels, door hardware power supplies, reader interface panels, branch panel boards with 20A 120 VAC security circuits, network switches, CCTV recorders, workstations, monitors, etc. Floor plans shall also show the conduit, raceway and/or cabling layout of the proposed routing between security devices, panels and central equipment locations.
    c. Security system details, customized for this project, showing junction and device box rough-in locations, conduit sizes, device mounting details, ADA required clearances and access routes, terminal strip locations and cabling requirements.
    d. Security device schedules and system component integration matrix.
    e. Security system Ethernet network riser diagram, including Owner's network

connection.

f. Security system RS485 and/or RS232 riser diagrams.

g. Order of Operations descriptions: Provide Sequences of Operation for the overall security system and for the operation of each controlled door and CCTV camera location. The sequences of operation shall be customized for this project and shall not be the manufacturer's standard descriptions for generic systems.

C. Close-Out Submittals

1. Provide software licenses, product keys, training guides, help-desk agreements and other related items to software and operating system administration.
2. Operation and Maintenance (O&M) Manuals, Record drawings, updated Product Data sheets, updated Shop Drawings (including updated calculations), updated Sequences of Operation, final test reports, warranty documentation, final network configuration files and training documentation.
3. Provide a complete and updated final list or bill of materials and equipment used on this project, including quantities, manufacturer, model numbers and a brief description of each item.
4. Provide electronic copies of all processed shop drawing documentation, including floor plans, details, schedules, wiring diagrams, schematics, risers and battery calculations.
5. Provide the final Sequences of Operation for the electronic access control and intrusion detection system and for the operation of each controlled door and opening, detection point including interface with Video Surveillance, Life Safety, Voice/Data services and other systems, as configured, tested and demonstrated.
6. Provide Contact information for the installer's representative and manufacturers' authorized factory representatives.
7. Provide the final system test reports, demonstrating that all devices, panels and equipment have been tested, individually and as a system, and that the system operates according to the sequences of operation, as outlined.
8. Provide a letter certifying that the security systems are installed entirely in accordance with the security systems manufacturers' recommendations and within the limitations of the required listings and approvals, that all system hardware and software has been visually inspected and tested by the manufacturers' certified representatives and that the systems are in proper working order
9. Provide executed warranties and service agreements.

D. MAINTENANCE SUBMITTALS

1. Spare Parts:
2. Extra Stock:
3. Tools:

E. QUALITY ASSURANCE

1. Qualifications
   a. Manufacturers: Equipment, components, products, materials and associated systems provided, including the Electronic Access Control System, or other similar or related systems shall be furnished by manufacturers who have been regularly engaged in the design and manufacture of these products for a period of not less than 5 years.
      1) Any manufacturer furnishing equipment, components, products or materials for this section shall directly design, manufacture or distribute the products specified in this document. The manufacturer's processes shall be monitored under a quality assurance program certified to ISO 9000 requirements.

2) All items furnished shall be employed in the Work for their intended purpose as listed by the manufacturer.

b. Installers Qualifications:
1) A firm certified by manufacturer of equipment and systems. Not less than three years relevant experience of successful design and installation of systems on projects of similar size and complexity.
2) The Intaller shall have integrated (or self-perform) engineering and project management capability consistent with the requirements of this project. The Installer shall provide qualified, trained and certified field technicians and tradespersons.
3) The installer shall engage representatives of the manufacturers furnishing items for this work in the detailed design and documentation, coordination of systems installation requirements and final system testing and commissioning.
4) The installer must be an authorized IDenticard business partner representative who shall be responsible for the satisfactory installation of the complete security management system, including the interface with the existing Loudoun County Government electronic access control and intrusion detention system.

c. Testing Agencies: The materials, appliances, equipment and devices shall be tested and listed by a nationally recognized and certified testing agency for use as part of a protected-premises protective access-control and intrusion detection system.
d. Certifications
e. Sustainablity Standards
f. Pre-Construction Testing

F. DELIVERY STORAGE AND HANDLING
1. Delivery and Acceptance Requirements
2. Storage and Handling Requirements
3. Packing Waste Management

G. FIELD/SITE CONDITIONS
1. Ambient Conditions
2. Dust and Debris Control

H. WARRANTY
1. The Manufacturer shall warrant all materials, products, components, equipment and systems for not less than one (1) year. Where the manufacturer's standard guarantee provides for a longer period, the longer period shall apply
2. The Installer shall warrant all materials, products, installation and workmanship for not less than one year
3. Extended Correction Period:

PART 2 - GENERAL

A. Equipment specified is intended as a reference standard for level of quality.

B. Provide materials listed by UL or ETL.

2.2 CONTROLLER

A. Specifications

1.	Alarm Inputs	(2) unsupervised, dedicated alarm inputs For enclosure tamper and power loss
2.	RAM Capacity:	1 MB, expandable by 3 MB to 4 MB total
3.	Visible	3 red, single-color LEDs
4.	Power to Standard Controller:	Twisted pair, 18 AWG (0.823 mm2)
5.	Port 1 – RS-485 or RS-232 to Host	RS-232:Twisted pairs, 22 AWG (0.325 mm2),with overall shield. Maximum cable length: 25 feet (7.6 meters) RS-485:Twisted pairs, 22 AWG (0.325 mm2),with shield, 120 ohms maximum. Maximum cable length: 4000 feet (1219 meters) of wire, total copper, including drops
6.	Ports 2-5	Twisted pairs, 22 AWG (0.325 mm2),with shield. Maximum cable length: 4000 feet (1219 meters) of wire, total copper, including drops
7.	Alarm Inputs	Twisted pair, 30 ohms maximum
8.	Connection to Relay-Controlled Devices	Use wire and gauge as required by load
9.	Connection to Input-Point Devices	One twisted pair per input, 30 ohms Maximum
10.	Connection to Readers	Refer to the reader manufacturer specifications for cabling requirements.
11.	Alarm Inputs	Twisted pair, 30 ohms maximum
12.	Port 1	RS-232,DTE, 9600; 19,200 or 38,400 Bps Two-wire or four-wire RS-485, 9600; 19,200 or 38,400 bpsPort 2 Two-wire RS-485: 2400 to 38,400 bps
13.	Ports 2 through 5	Two wire RS-485 2400 to 38,400 bps
14.	Standard Controller Input Voltage	12 VDC ± 10%,350 mA
15.	Memory and Clock Backup	Lithium coin cell,3.0 V, type BR2325,BR2330,CR2330
16.	Temperature	32°F to 158°F (0°C to 70°C) operating -67°F to 185°F (-55°C to 85°C) storage
18.	Relative Humidity	0 to 95% RH noncondensing

B. Acceptable Manufacturers

1. Identicard PremiSys CTLRSTD. Provide quantity and configuration as required to support quantity of doors shown on plans.
2. No Substitutions

2.3 TWO-READER BOARD

A. Specifications

1.	Inputs – Dedicated	Two unsupervised, dedicated input

		points for enclosure tamper and power loss
2.	Inputs – Assignable	Eight input points, end-of-line (EOL) resistors,1K/1K ohm 1% ¼ watt standard
3.	Relays	Six relays con$gurable for normally open or normally closed operation
4.	Relay Contact Type	Form C
5.	Relay Configuration	Single-pole double-throw (SPDT)
6.	Visible	Twenty red, single-color LEDs
7.	Power to Two-Reader Board	One twisted pair, 18 AWG (0.823 mm2)
8.	RS-485 Connections to Controllers	Twisted pairs, 22 AWG (0.325mm2), with shield Maximum cable length: 4000 feet (1219 m) of wire, total copper, including drops
9.	Connection to Relay-Controlled Devices	Use wire and gauge as required by load
10.	Connection to Input-Point Devices	One twisted pair per input, 30 ohms Maximum
11.	Connection to Readers	Refer to the reader manufacturer specifications for cabling requirements. Maximum cable length: 500 feet (150 m), total copper, including drops
12.	Two-Reader Board Input Voltage	12 VDC ± 10%, 550 mA peak (plus reader current),450 mA (plus reader current) nominal
13.	Relay Rating (each of six relays)	5 A at 28 VDC, noninductive load
14.	Card Reader Power (each of two readers)	12 VDC ± 10% regulated, 125 mA max. each reader, or 12-24 VDC ± 10% (input voltage passed through),125 mA max. each reader; min. 20 VDC as input needed to yield 12 VDC at reader port
15.	Reader LED Output	TTL-compatible; high > 3 V, low < 0.5 V; 5 mA source/sink maximum
16.	Reader Data Inputs	TTL-compatible inputs
17.	Board Width	8.0 inches (203 mm)
18.	Board Height	6.0 inches (152 mm)
19.	Board Depth	1.0 inch (25 mm)
20.	Temperature	32°F to 158°F (0°C to 70°C) operating -67°F to 185°F (-55°C to 85°C) storage
21.	Relative Humidity	0 to 95% RH noncondensing

B. Acceptable Manufacturers:

1. Identicard PremiSys PREM-BRD2RDR
2. No Substitutions

2.4 INPUT BOARD

A. Specifications

1.	Inputs – Dedicated	Two unsupervised, dedicated input points for enclosure tamper and power loss
2.	Inputs – Assignable	Sixteen input points, end-of-line (EOL) resistors,1K/2K ohm 1% watt standard
3.	Relays	Two relays con$gurable for normally open or normally closed operation
4.	Relay Contact Type	Form C
5.	Relay Configuration	Single-pole double-throw (SPDT)
6.	Power to Input Board	One twisted pair, 18 AWG (0.823 mm2)
7.	RS-485 Connection to Controller or MUX:	Twisted pairs, 22 AWG (0.325mm2), 120-ohm impedance with shield. Maximum cable length: 4000 feet (1219 m) of wire, total copper, including drops
8.	Connection to Relay-Controlled Devices:	Use wire and gauge as required by load
9.	Connection to Input-Point Devices:	One twisted pair per input, 30 ohms Maximum
10.	To Controller or MUX	Two-wire RS-485, via TB1, 2400 to 38,400 bps
11.	Input Board Input Voltage	12 VDC ± 10%, 350 mA peak, 300 mA Nominal
12.	Relay Rating (each of two relays)	5 A at 28 VDC, noninductive load
13.	Board Width:	8.0 inches (203 mm)
14.	Board Height	6.0 inches (152 mm)
15.	Board Depth	1.0 inch (25 mm)
16.	Temperature	32°F to 158°F (0°C to 70°C) operating -67°F to 185°F (-55°C to 85°C) storage
17.	Relative Humidity	0 to 95% RH noncondensing

B. Acceptable Manufacturers:

1. Identicard PremiSys PREM-BRDIN
2. No Substitutions

2.5 OUTPUT BOARD

A. Specifications

1.	Inputs – Dedicated	Two unsupervised, dedicated input points for enclosure tamper and power loss
2.	Relays	Sixteen relays con$gurable for normally open or normally closed operation
3.	Relay Contact Type	Form C
4.	Relay Configuration	Single-pole double-throw (SPDT)
5.	Power to Output Board	One twisted pair, 18 AWG (0.823 mm2)

6.	RS-485 Connection to Controller or MUX:	Twisted pairs, 22 AWG (0.325mm2), 120-ohm impedance with shield. Maximum cable length: 4000 feet (1219 m) of wire, total copper, including drops
7.	Connection to Relay-Controlled Devices	Use wire and gauge as required by load
8.	Connection to Input-Point Devices	One twisted pair per input, 30 ohms Maximum
9.	To Controller or MUX	Two-wire RS-485, via TB1, 2400 to 38,400 bps
10.	Output Board Input Voltage	12 VDC ± 10%, 1100 mA peak, 850 mA Nominal
11.	Relay Rating (each of 16 relays)	5 A at 28 VDC, noninductive load
12.	Board Width	8.0 inches (203 mm)
13.	Board Height	6.0 inches (152 mm)
14.	Board Depth	1.0 inch (25 mm)
15.	Temperature	32°F to 158°F (0°C to 70°C) operating -67°F to 185°F (-55°C to 85°C) storage
16.	Relative Humidity	0 to 95% RH noncondensing

B. Acceptable Manufacturers:

1. Identicard PremiSys PREM-BRDOUT
2. No Substitutions

2.6 ENCLOSURE

A. Specifications

1.	Enclosure Width	18.19 inches
2.	Enclosure Height	21.38 inches
3.	Enclosure Depth	4.56 inches

B. Acceptable Manufacturers

1. Identicard PremiSys PREM-ENCLG
2. No Substitutions

2.7 ACCESS MANAGER SOFTWARE - SERVER

A. Specifications

1. Installation and Licensing

   a. The County owns an existing enterprise license for the access control software. Coordinate all software licensing with the County.

2. Communications: Host

   a. The system controllers shall confirm receipt of all commands from the PC to ensure

that no system transactions are lost.

b. The communications between the host and connected controllers shall be continuously monitored with the host initiating all message exchange sequences. Supervision of system input points shall be provided by the controller. Failure or fault of data connections between the controller(s) and server(s) shall be indicated on the system display on a User Interface PC.

c. It shall be possible in the system to require controllers to confirm with the host computer and its cardholder database that a card presented is a valid card. The host shall respond with a command either to confirm that access should be granted or to deny access, based on information in the cardholder database resident in the host. If this option is not enabled, the normal action of the card presentation being verified against the database on the controller shall be in effect. If this option is implemented in a system, users shall be able to define a timeout value, that is, a length of time that controllers shall wait for the host to respond. If the host does not respond within this set time, the controller shall function normally to either grant access or to deny it.

d. It shall be possible to easily update firmware files on any controller and/or reboot the processor in any controller via software commands from the host.

3. Communications: Components

a. The software shall support a maximum of 254 channels per system and a maximum of 8 controllers per channel.

b. The system hardware shall support various communication methods for communication among host computers, controllers and I/O components. It shall be possible to use serial RS-232 or serial RS-485 methods as well as TCP/IP over Ethernet methods, with dependence on the communications specifications of the individual controllers. Communications among controllers and I/O boards connected to them shall be via serial RS-485.

c. It shall be possible for system users to define the number of times the host attempts to retry to connect to a controller before the controller is considered offline by the system. The range of times shall be from 0 to 32,767.

d. System integrators shall be able to enable or disable communication to individual I/O boards and select the speed to communication between each. The baud rate of communications among the controllers and I/O boards shall be user-selectable from among the following: 2400; 9600; 19,200 and 38,400. If legacy IDenticard® Series 9000™ hardware is incorporated into the system a specific baud rate must be used (see Legacy Hardware paragraph below).

4. Legacy Hardware

a. The software shall allow the integration of legacy IDenticard® Series 9000™ Panels (with or without optional Reader Expansion Cards) and/or Remote Input/output (RI/O) boards. When these components are incorporated into the access control system, the panels shall appear in the software as reader boards and the RI/Os as input and output boards. If the software is installed in a system that includes this hardware, the baud rate for any controller communicating to these I/O components shall be 9600 only.

5. System Security and User Rights

    a. For each application-level user of the system, it shall be possible for the administrator to define the user name, enter the full first and last names of the user, define a password, and enter an e-mail address. It shall also be possible to establish activation and expiration dates for the user account in the system. Passwords permissible for use in the software shall conform to default Windows® requirements.
    b. It shall also be possible for the administrator to use the network user names and passwords of LDAP users.
    c. When the software opens, a login window shall appear and prompt the operator to enter his or her system user name and password. If the login attempt fails, the software shall indicate the nature of the failure, i.e., incorrect password or invalid user name. In addition, each time that this login window appears, it shall display the user name of the last user to log into the system on that computer.
    d. The software shall include a system-administration application that allows administrators to manage operator accounts. Administrators shall be able to create groups having specific assigned rights and then to add operators to these groups and manage these groups. The administrators may edit any settings regarding an operator, in accordance with their own administrative rights within the system.
    e. It shall be possible to specify particular cardholder record screens to open by default when a specific operator opens a cardholder record without choosing a particular data- entry screen to use.
    f. The software shall enable administrators to assign time periods to users, which determine the days and times during which group rights are valid. Time periods can be associated with groups or users. Operators shall be able and need to enter a unique name as part of the definition of any time period.
    g. The software shall provide a method to limit the cardholder records a user may view and modify, in accordance with other system permissions. This method, termed cardholder filtering, allows the security administrator to create criteria to filter cardholder records and then assign the cardholder filter to groups of users so that only the records that meet the criteria are displayed for the logged-in users. If no such filter is assigned to a group of users those users shall be able to view all cardholders in the system unless the user belongs to another group that is assigned a cardholder filter. The software shall also provide a means by which users in a group can always see all cardholders; cardholder filtering shall not apply to them.

6. User Interface

    a. The User Interface shall incorporate a menu bar with drop-down menus and display icons for full system setup and operation. This menu and these icons shall offer to system users' complete access on one screen to all system functions and system setup parameters to which the users have rights. Users shall be able to design, store and display multiple, individually created screens used to display cardholder information and data. The system shall support an unlimited number of operator defined screen layouts that shall accommodate the data fields in the system. The system shall additionally be built and delivered with a standard, ready-to-use data-entry screen. This product-standard screen shall be able to be modified and saved

under a new screen name by the operator.

b. The user interface shall provide windows and other controls for viewing system cardholder activity; monitoring and acknowledging alarms; and monitoring and controlling input points, relays and door configurations.

c. A data-entry screen shall be assignable to a system user for automatic display when that user logs in. It shall be possible to define default screens that always appear when a particular user logs onto the system. The system software shall allow an authorized user to select an appropriate screen layout from a menu on a per-client interface basis.

7. User Interface

a. The User Interface shall incorporate a menu bar with drop-down menus and display icons for full system setup and operation. This menu and these icons shall offer to system users' complete access on one screen to all system functions and system setup parameters to which the users have rights. Users shall be able to design, store and display multiple, individually created screens used to display cardholder information and data. The system shall support an unlimited number of operator defined screen layouts that shall accommodate the data fields in the system. The system shall additionally be built and delivered with a standard, ready-to-use data-entry screen. This product-standard screen shall be able to be modified and saved under a new screen name by the operator.

b. The user interface shall provide windows and other controls for viewing system cardholder activity; monitoring and acknowledging alarms; and monitoring and controlling input points, relays and door configurations.

c. A data-entry screen shall be assignable to a system user for automatic display when that user logs in. It shall be possible to define default screens that always appear when a particular user logs onto the system. The system software shall allow an authorized user to select an appropriate screen layout from a menu on a per-client interface basis.

8. Access Control Cards

a. The system shall allow data to be entered to stipulate dates for the following parameters: card-activation dates, card-deactivation dates, vacation-start dates and vacation-end dates.

b. It shall be possible in the software to designate a cardholder as exempt from area tracking for anti-pass back purposes. In addition, cardholders' records can include settings that allow them to benefit from extended time at doors and readers as specified under the Americans with Disabilities Act.

c. The system shall allow a user to copy a cardholder's card settings to create an additional card for that cardholder. All card settings other than the card number are copied to the additional card.

d. The system shall allow a user to reassign a cardholder's card settings to create a new card for that cardholder. All card settings other than the card number are copied to the new card.

e. The system shall provide the means to assign multiple access control cards to a single cardholder record so that the user is not required to enter duplicate

cardholder information for each card.

9. Block Add for Cardholders with Cards

    a. The system shall provide the means to add a block of cardholder cards in such a way that each card is assigned a card number unique within the system. The user shall be able to select the number of cardholder records to be created in the system. The user shall be able to select a starting number for the block of cards so that card numbers in the system can be reused. The means shall exist to overwrite cards with the same number and reassign those numbers to the new cardholders if the user selects the option.
    b. The system shall provide the means to assign the same settings to all cards for the following fields: activation and inactivation dates; vacation start and end dates; use count settings to be used with use limits as outlined elsewhere in this specification; antipassback settings to be used with antipassback as outlined elsewhere in this specification; ADA (Americans with Disabilities Act) timing settings; access groups as outlined elsewhere in this specification; user levels as outlined elsewhere in this specification. Systems incapable of creating large blocks of cards with such time-saving card-creation capability shall be deemed unacceptable.

10. Importing Legacy Product Cardholders' Card Data

    a. It shall be possible to use the Data Importer (see related specification) to import specific cardholders' card data from legacy IDenticard IDentiPASS™ access control systems into the specified access control system. Via the Data Importer, the user shall be able to import the following information from the legacy system: the card number; whether the card is active or inactive; any PIN assigned to the card; an activation date and/or time; a deactivation date or time; and whether the card is antipassback-exempt.

11. Global Access Groups

    a. The software shall permit the configuration of access groups that consist of doors and/or elevators from multiple controllers and sites. Such access groups shall be termed "Global Access Groups." It shall be possible to create up to 32,000 global access groups in the system.
    b. It shall be possible to establish up to 32 access groups per cardholder per controller that designate the permissible readers that cardholders may use and the time zones, or schedules, during which they may be used. By defining the permissible readers, the areas to which each cardholder has access rights shall thereby be defined. This definition of access rights in the system shall allow access to any cardholder if a particular time zone is active at a particular reader, that reader is part of the access group, and all other access- rights tests prove valid for that cardholder.
    c. Administrative users of the system shall be able to control which users of the system are permitted to create and delete global access groups, and to assign global access groups to cardholder cards, These permissions shall be applied on a user-group basis, and so provide the capability to "filter out" specific access groups from view and use by specific users when they are logged into the system.
    d. Through the use of the elevator access groups, it shall be possible to define elevator

operation for normal business hours, operation after hours, on weekends and during special events. It shall be possible as well to define a "default" floor-access scheme that controls the access of non-cardholders (where applicable).

e. The software shall provide a means by which users can remove one or more doors and/or elevators from all global access groups in the system.

f. A warning message shall appear to the User when assigning a particular access group to a card causes the limit of 32 access groups per cardholder per controller to be exceeded.

g. A warning message shall appear to a second user who attempts to save configuration changes to an access group that was previously opened by another user and is still open for viewing or editing by that first user. This warning shall alert the second user that his or her modifications to the access group shall not be saved. It is the first user's changes that are saved. The second user shall be free to configure his or her settings at a later time after the first user has finished configuration.

12. Anti-Pass back, Areas, Occupancy

a. The software shall permit the configuration and use of several forms of antipassback including:

b. Reader-based antipassback, which shall prevent the same card from being used at the same reader within a defined space of time. If a card is presented more than once before the defined time has elapsed, presenting the card shall not permit access to be granted.

c. Area-based antipassback, which shall allow "tracking" of entries into and exits out of defined areas. These area designations shall correspond to an area reference and shall be assigned to door configurations in the software. The door shall have a defined area in which it is located and a defined area into which the door leads. "Hard" antipassback rules shall prevent the user from moving between areas without using the card reader. "Soft" rules shall permit access when those rules are violated, while recording the antipassback violation as a transaction.

d. It shall be possible to "reset" an individual cardholder's antipassback status whenever desired, by granting a "free antipassback pass" to the cardholder, as well as to globally grant "free antipassback passes" that apply to all cards downloaded to a specific controller.

e. Means shall exist in the software to configure up to 128 access areas per controller, these areas being used for antipassback configuration and other features as described below.

f. It shall be possible by these means to require the number of cardholders in any access areas to be no fewer than two.

g. It shall be possible, through a separate function in the software, to set a maximum number of cardholders who are allowed in any area. The software shall be able to generate an alert in the form of a transaction on a client computer as a maximum occupancy value is approached. The software shall also be able to generate a similar alert as a defined near-minimum value is approached.

h. The system shall be capable of saving the time, date and access-control reader number of the last entry for all cardholders as they move through the access-controlled facility for the purpose of antipassback.

13. Use Limits

    a. It shall be possible to define for any card in the system a set number of times that the card can be used at readers configured to count card uses. The number of uses remaining on a card shall be decremented when the card is presented for access at a reader that is configured to be used to implement this feature. It shall be possible to require any system reader to decrement a use count for a card. It shall be equally possible for a card to be used at readers that do not decrement the use count of that card.

14. Holidays and Time Zones

    a. There shall be no limit on the number of time zones and holidays defined in the system other than limits imposed by the amounts of memory allocated and used in controllers in the system.
    b. It shall be possible to define blocks of time over the course of one or more days - up to seven days per calendar week - that are used for controlling access and initiating or halting automated operations. These blocks of time are termed time zones and shall consist of one to six individual time intervals that are set to span various hours of the day.
    c. It shall be possible to activate or deactivate time zones based on triggers or procedures defined elsewhere in the system software. It shall also be possible to temporarily alter or override time zones using direct commands and/or holidays - days during which the interval is disabled. An inactive time zone shall be automatically activated at the moment any of its intervals becomes active (reaches its start time). An active time zone shall be automatically deactivated at the moment its last active interval becomes inactive (elapses past its end time). Via a direct command from the host to a controller, users shall be able to activate an inactive time zone and deactivate an active time zone, or a time zone can be allowed to return to its normal state (release from override). Users shall also be able set the time zone override to persist until the next direct command, or it can be set to resume automatic control the next time the interval status changes.
    d. Holidays shall be configurable in the system to specify exceptions to the day-of-week schedules defined for any time zone. In this way, the holiday shall provide a break in the schedule the time zone creates. Holidays shall be definable by the date and duration of the holiday and its type. It shall be possible to create system holidays that span more than one day. The maximum number of days that can be set up for holiday duration is 32,767. The holiday type shall be used to group holidays together and to designate schedules that are active when a holiday of a certain type occurs. When a holiday is active, it shall supersede the normal time-zone interval settings.
    e. It shall be possible to configure a holiday in such a way as to override all time zones in a system and essentially disable most granting of access and all time-zone dependent functions. In addition, by the assignment of holiday types to intervals in a time zone, it shall be possible to cause the holiday to be in effect for only a portion of a day, allowing partial-day holidays.

15. Daylight Saving Time

    a. Users shall be able to allow for worldwide time zone offsets and daylight saving time offsets on an individual controller basis. The controllers shall be able to hold 20 date pairs for daylight saving time, allowing the creation of a 20-year span of current and future daylight saving time schedules.

16. Duress Codes

    a. The system shall allow the configuration and use of duress codes. Duress codes shall consist of modifying current card numbers in such a way as to make them unique to each cardholder and recognizable system-wide. A duress code that is the same for all cardholders in a system shall be deemed unacceptable. It shall also be possible to deny access to an entered duress code on a reader-by-reader basis.

17. Card Formats

    a. Users shall be able to select ABA and Wiegand reader card formats. Up to eight card formats shall be selectable per reader. The software shall accommodate multiple formats to allow the use of badges with different facility codes or different data lengths. These card data formatting capabilities shall allow the use of different reader technologies without modification to the software. The system shall support readers (with or without keypads) using magnetic-stripe, proximity, smart-card and biometric technologies.
    b. The software shall allow the configuration of multiple card formats to allow the use of badges with different site/facility codes and/or different data lengths. The maximum value for a facility code shall be 32 bits.
    c. The system shall support the use of cards with Wiegand or ABA formats, to accommodate magnetic-stripe, bar-code, smart-card, proximity and other cards.
    d. The software shall work with a unique identifier block on the identification card that contains a cardholder ID of up to 19 digits (64 bits), an optional issue code to uniquely identify lost and reissued cards and an optional PIN of up to 15 digits.

18. User Levels

    a. The software shall allow individual card records to be designated so that selected controller triggers can be linked to those cards. These designations are termed user levels and shall be provided to enable cardholder cards to be used as triggers in triggers and procedures as defined in this specification. It shall be possible to establish in the software up to 256 user levels, which shall then be capable of being assignable to individual cards. It shall also be possible to assign up to seven user levels to a single card. The software shall allow a single user level to be assigned to more than one card or cardholder. The user shall as well be able to define specific doors within a group of doors at which the triggers shall work.

19. Auto Photo Recall

    a. The system shall provide the means to display a cardholder photo on the system-monitoring screen when the cardholder presents a card at a system reader. The

default display is a grid with the most recent cardholder photo in the top left corner and the previous 11 photos displayed as smaller versions in three rows.

b. Users shall be able to create customized photo recall configurations using one of the following layouts: a basic 1x8 grid with all 8 photos the same size; a basic 2x8 grid with all 16 photos the same size; an advanced 3x8 grid with the most recent photo in the top left portion of the screen and the other 20 photos displayed as smaller versions in three rows; an advanced 3x5 grid with the most recent photo in the top left portion of the screen and the other 11 photos displayed as smaller versions in three rows; an advanced 4x5 grid with the two most recent photos in the top left and middle portions of the screen and the other 12 photos displayed as smaller versions in the four rows; an advanced 5x8 grid with the two most recent photos in the top left portion of the screen and the other 2 photos displayed as smaller versions in five rows.

c. Users shall be able to specify the door and/or elevator readers that shall cause a specific customized photo recall layout to display when monitoring and controlling the system. The system shall allow a combination of any or all doors/elevators to be selected in the configuration for the customized layout and such doors/elevators can be from any part of the system.

d. The system shall provide the means to display additional cardholder and card information in a details section of the photo recall display. The specific database fields containing the information shall be selectable by the user upon configuration of the customized photo recall display, including but not limited to the first and last name, card number, phone number, department and automobile information.

20. Alarm Acknowledgements

a. The software shall provide for alarm management capabilities. It shall be possible to set up system transactions or events to require alarm acknowledgement. The system shall provide user-defined alarm-handling capabilities to include easy-to-use interfaces to create alarm acknowledgement alert messages, acknowledgment response options and priority parameters, and password and comment requirements. Alarm management shall also provide for removing alarm acknowledgements from the User's display.

b. It shall be selectable by the Owner/User or administrator to display the alarm-acknowledgement window, and which types of transactions are to be displayed shall be selectable as well. The alarm acknowledgement window shall be capable of showing all of the columns that appear in the monitor transactions window, and also allow the filtering of specified transactions, the selection of columns to display and the selection of column widths.

c. Fifty user-nameable priority levels shall be available to denote the severity of alarms. Assignment of priority levels to alarms shall provide options to require users to enter notes, usernames and/or passwords to acknowledge and/or clear alarms. The software shall also give users options to acknowledge or clear alarms in one step with a single click of a button. Users' capability to acknowledge and/or clear alarms and the method they may use are determined by permissions assigned in the security administration module of the software to users like any other permission.

d. It shall be configurable in the software to cause the alarm acknowledgement

window to immediately appear "on top" of any other Windows® application running on the system computer. The system shall offer means to users to select predefined responses to describe the handling of a particular alarm. These predefined responses shall be configurable in the alarm acknowledgement module.

e. The software shall provide a default sound for all alarm acknowledgment alarms. The user may optionally select customized sounds for use with specific alarm acknowledgment priority levels or triggers. The alarm sound for the highest priority level alarm shall "loop" continuously until the alarm is acknowledged and then the next highest priority level alarm will sound.

21. Global Triggers and Procedures

a. The software shall permit the configuration of triggers and procedures that consist of points from multiple controllers and sites. Such triggers and procedures shall be termed "Global Triggers and Procedures." The user shall be able to choose whether to configure the individual elements of a trigger and procedure (actions, action groups, procedures and triggers) on an element-by-element basis or to make use of a software wizard that streamlines the configuration process.

b. The software shall provide customizable means by which users can choose an event in the system to trigger an action that the system takes. These triggers and procedures shall provide a means for event-based control as opposed to solely time-based control, although the starting and ending of time zones can be used as triggers. It shall be possible, through the use of user levels as described in this specification, to use card- generated transactions and/or system events as triggers.

c. Procedures shall be available and consist of any configurable system action to be taken in response to the triggering event. Procedures shall have sufficient flexibility so as to permit the configuration of a virtually unlimited number of system actions that can be applied to many procedures. The software shall allow, per controller up to 4096 individual actions to be included in one global action group; up to 4096 global action groups to be incorporated into one global procedure (or a limit of four action groups per procedure, if the action groups are not to cross controllers or sites); and up to 4096 global procedures. There shall be no restriction beyond the system limit given above on the number of action groups in which a single action can be included.

d. It shall be possible when configuring procedures to include a time-delay feature that shall allow the actions of the procedure to temporarily pause. The pause shall be user- configurable from 0 to 16384 seconds. Such action delays shall allow for another action to occur in the system before the system resumes the action of the paused procedure. It shall be possible to abort paused procedures during these action delays. Systems not allowing the configuration of such delay times shall be deemed unacceptable.

e. The elements of triggers and procedures – triggers, procedures, action groups and actions shall be represented in the software by icons in their relevant configuration windows. Whenever any of these elements contain actions or points that cross controllers, these global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them.

f. Means shall be provided in the trigger-configuration window to allow users to edit

or create time zones as defined elsewhere in this specification. These means permit "on-the-fly" editing or creation of time zones when choosing the time zone during which the trigger can occur and/or when choosing a time zone that is to act as a trigger.

22. HARDWARE CONFIGURATION

a. Through the software application, users shall be able to view the firmware version numbers of any controller in the system.
b. Through the software application, it shall be possible to view the total amount of memory installed in any controller as well as the amount of free memory available for use.
c. It shall be possible for system users to define the number of milliseconds between messages from the host before a controller is considered offline by the system. The range of milliseconds shall be 10,000-65,000.
d. The system shall support the connection of a virtually unlimited number of controllers when connecting controllers using Ethernet. When connecting via Ethernet the only limits are those imposed by the user's PC memory and speed, network bandwidth and/or IP addresses available for use on the user's network. It shall be possible to connect up to 8 controllers in a "multidrop" configuration per RS-485 serial channel. It shall also be possible to connect one controller per RS-232 serial channel.
e. It shall be possible through the software to disable individual I/O boards in the system for any reason.
f. The hardware boards to which readers are connected shall indicate and generate a transaction in the system if a "forced-open" or "door-ajar" are detected at the door/reader connected to the hardware board.
g. When configuring any item of hardware it shall be possible in the system software to choose the settings of a particular item as the settings "template" that is used by default for the settings of all other items of the same type. The user has the capability of temporarily disabling this choice at any time and then later re-enabling it if desired. Systems incapable of enabling, optionally disabling and optionally re-enabling settings in this manner shall be deemed unacceptable.

23. Doors and Reader Settings

a. It shall be possible to connect controllers to reader boards so that the system has a maximum of forty (40) readers, including those readers attached to controllers with onboard reader ports.
b. When inputs change state virtually simultaneously, they shall normally be processed sequentially from low input-point numbers to high numbers on any I/O board. However, the software shall provide a setting to reverse the processing sequence of two input points wired as door-position and request-to-exit points to prevent the processing of information in the incorrect order when these two inputs appear to change simultaneously. For example, if the REX input is wired to a higher point number than the door status (door- position input point), the door-open event is processed before the REX, and so the system reports that the door was forced open (the door opens before the REX is received). This setting changes the order in

which these two inputs are processed, to report the events in the proper order.

c. The software shall be capable of permitting readers to support the following basic reader access modes: unlimited access; exit only, no entrance access; disabled; access on valid facility code alone; access on valid card number alone; access on valid PIN code alone; access on valid PIN code AND card number; access on valid PIN code OR card number.

d. The system shall be capable of generating a transaction indicating whether a controlled door was opened and used after a valid card is read and the associated door unlocked.

e. The system shall permit the configuration and use of master and slave readers for use as, for example, "in" and "out" readers for antipassback. The slave reader shall make access requests to the master reader, and the two readers are handled by the software as a single reader.

f. It shall be possible to activate the relay controlling a door lock for a range of time from 1 to 255 seconds, in one-second increments. It shall also be possible to configure a door- lock relay to energize when activated (termed the "Normal" mode) and to de-energize when activated (termed the "Inverted" mode). In addition, it shall be possible to allow the door to relock as soon as the door opens or upon the door closure.

g. The reader port, door-position-input point and the request-to-exit input point (REX) for a reader-door shall be established by default, when the automatic generation of doors is selected as a part of reader-board setup; however, users of the system shall be able to easily redefine any request-to-exit input point they need.

h. The system shall allow alternate readers to be set up to work concurrently with another reader to control one door. An alternate reader shall be useful, for example, as a reader placed higher than the main reader at a parking lot entrance for use by truck drivers whose vehicles are taller than passenger cars.

i. It shall be possible to select in the system whether it is desired to log a transaction indicating that access was granted to a cardholder before the system verifies that the door was actually used. Select this option so that as soon as access is granted, a transaction is logged indicating that the cardholder accessed the area, whether or not the door was used.

j. The system shall allow doors to be configured so as not to energize the door-lock relay upon a REX.

k. The system shall allow doors to be configured so as not to display all change-of-state transactions occurring at the door.

l. The system shall allow doors to be configured so as to require two cards to be presented within 10 seconds of each other at the door's reader for the cardholders to enter or exit.

m. Cardholders shall be able to use the keypad to enter the card numbers at doors that have been configured in the software to allow direct entry of card numbers at keypad readers.

n. It shall be possible to select from three different sets of default settings to control LED action on readers so enabled.

o. The system shall be capable of generating pre-alarm transactions that can serve as alerts that a door is about to go into a door-ajar state. It shall be possible in the software to specify a defined number of two-second units at which the pre-alarm should be generated before the door goes into the door-ajar state.

p. It shall be possible to select an antipassback delay to apply to any reader configured for time-dependent antipassback. The range of values in seconds that can be selected is 0-255, in one-second increments.
q. The system and software shall support the configuration of separate setups for readers and doors so as to comply with requirements provided for under the Americans with Disabilities Act (ADA).
r. It shall be possible in the software to choose alternate door-strike time and held-open time for use as part of a "special door cycle" for ADA compliance. This door-strike time shall range from 0 seconds through 255 seconds. The held-open time shall consist of specifying the number of two-second ticks, and the number of ticks is selectable from the range of 0 through 32757.
s. It shall be possible for the system to log card presentations in a transaction log at a reader which is in an unlimited-access mode.
t. The user shall be able to create global access groups that pair the access-controlled doors of the building with system time zones to specify the doors at which cardholders are permitted access and at which times of the day and days of the week.

24. Monitor Points and Monitor Point Groups

a. Input points shall have standard supervision configurations that allow the input to be wired normally closed or normally open, or to be wired with selective resistance on the point to allow 1000 ohms resistance as the normal state and 2000 ohms as the active state or 2000 ohms resistance as the normal state and 1000 ohms as the active state.
b. Users shall be able to configure custom de-bounce times and motion-detector delays in the system. The number of successive input scans (de-bounce) shall have the range of 2-15, and the range of possible motion-detector delays shall be 0-15.
c. The system shall allow the "masking," or shunting, of monitor points to suppress event reporting for changes between active and inactive input conditions. However, it shall be possible as well to allow users to select an option to report changes even when inputs are masked.
d. The software shall allow the selection of latching and non-latching input-point modes. The latching mode causes a door-position input point to go into alarm once a door is opened, regardless if the door is shut again, unless the monitor point is masked. Non-latching mode prevents the alarm event from being generated when the associated door is opened and then immediately closed (within the entry delay).
e. The system shall accommodate both entry and exit delays with respect to arming and disarming monitor points. Users shall be able to configure the amount of time an alarm is to be delayed after an entry to allow authorized personnel to disarm monitoring points after that entry. Users shall also be able to configure the amount of time alarms are to be delayed after the alarm system is armed to allow authorized personnel to exit an area without setting off alarms.
f. Users shall be able to create a monitor point group consisting of a mixture of monitor points and doors from the same controller such that the status of the group can be monitored and specific settings changed "on-the-fly" through a monitor and control means as described in this specification.

25. Control Points

a. It shall be possible to set the output points (relays) used as control points to have "normal" or "inverted" action, as described in this specification.
b. The system shall allow the following control-point (non-door-lock relay) actions: off; on; single pulse of 0-100,000 seconds; or repeated pulse with on-times and off-times in .1 second steps and a selectable repeat count; all repeated-pulse settings range from 0 to 255.

26. Global Monitor Point Groups

a. The software shall permit the creation of global groups of monitor points. Users shall be able to select monitor points from any site in the system to create a global monitor point group. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of points in the group shall be able to be changed "on-the-fly" through a monitor and control means as described in this specification.
b. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

27. Global Control Point Groups

a. the software shall permit the creation of global groups of control points. Users shall be able to select control points from any site in the system to create a global control point group. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of points in the group shall be able to be changed "on-the-fly" through a monitor and control means as described in this specification.
b. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

28. Global Door Groups

a. The software shall permit the creation of global groups of doors. Users shall be able to select doors from any site in the system to create a global door group. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of the doors in the group shall be able to be changed "on-the-fly" through a monitor and control means as described in this specification.
b. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

29. Monitoring and Controlling – Access Areas

a. Users shall be able to modify access-area settings during regular operation (as opposed to during configuration) to enable or disable the access area or to modify the current occupancy value.
b. In the right-hand pane of the Monitor and Control tree window, the user has the

option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

30. Monitoring and Controlling – Time Zones

    a. The software shall allow time-zone actions to be overridden in the following ways: temporarily deactivate the time zone until it would normally change, temporarily activate the time zone until it would normally change, deactivate the time zone until a later overriding command, activate the time zone until a later overriding command; return the time zone to normal, log the time zone state in the transaction log.
    b. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

31. Monitoring and Controlling – Antipassback

    a. The software shall permit the generation of commands that disable antipassback restrictions.
    b. These commands shall be selectable for application on a per-cardholder basis or for all cardholders in the system.
    c. This command shall act as a way of (re)initializing users for area- based antipassback, as described in this specification. After the issuance of this command, which essentially acts as a "free pass" for antipassback, the movements of the affected cardholder(s) are logged and stored by the system. The issuance of this command for all cardholders shall allow all cardholders to be resynchronized with respect to antipassback. Additionally, the software shall permit the generation of a command that moves a cardholder's location to a specific area, on a per cardholder basis.
    d. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

32. Monitoring and Controlling – Doors

    a. The software shall allow users to send commands to a door in the system through a system "monitor and control" means in such a way that the door can be momentarily unlocked. The door still shall be monitored for door-ajar conditions, and any granted cardholder access that occurs during this time will be logged.
    b. It shall be possible to change the mode of a door "on the fly" through a system "monitor and control" means in such a way that the following reader modes can be achieved: unlimited access; exit only with no entrance; disabled; access on valid facility code alone; access on valid card number alone; access on valid PIN code alone; access on valid PIN code AND card number; access on valid PIN code OR card number.

c. Users shall be able to send commands to a door through a system "monitor and control" means in such a way that the door-position input can be set to mask or unmask (disarm or arm, respectively) the specific door point. Setting a mask suppresses alarm conditions when the input is active, and clearing the mask restores the "visibility" of the alarm in the system. It shall also be possible to view the status of the door, that is, whether or not the door-position input is active and whether or not the point is masked, through this "monitor and control" means.
d. Users shall be able to send commands in the system in such a way that the "door forced open" events at any door are "masked," that is, the generation of these events is suppressed. Users shall be able to send commands in the system in such a way that the "door-ajar" events at any door are "masked," that is, the generation of these events is suppressed.
e. Any changes made to door settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the controller's database are downloaded to that controller with the original hardware configuration settings.
f. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

33. Monitoring and Controlling – Global Door Groups

a. The software shall allow users to send commands to a global group of doors in the system through a system "monitor and control" means in such a way that all doors in the global group can be momentarily unlocked. The doors still shall be monitored for door-ajar conditions, and any granted cardholder access that occurs during this time will be logged.
b. It shall be possible to change the mode of all doors in the global group "on the fly" through a system "monitor and control" means in such a way that the following reader modes can be achieved: unlimited access; exit only, no entrance access; disabled; access on valid facility code alone; access on valid card number alone; access on valid PIN code alone; access on valid PIN code AND card number; access on valid PIN code OR card number.
c. Users shall be able to send commands to all doors in the global group through a system "monitor and control" means in such a way that the door-position input can be set to mask or unmask (disarm or arm, respectively) the door points in the global group. Setting a mask suppresses alarm conditions when the inputs are active, and clearing the mask restores the "visibility" of the alarms in the system.
d. Any changes made to settings for the doors in the global group using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the controller's database is downloaded to that controller with the original hardware configuration settings.
e. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

34. Monitoring and Controlling – Monitor Points

    a. The software shall allow users to send commands to a selected monitor point in the system through a system "monitor and control" means. These commands shall consist of setting or clearing the mask (disarming or arming, respectively, the point) for the specific monitor point. Setting a mask suppresses alarm conditions when the input is active, and clearing the mask restores the "visibility" of the alarm in the system. It shall also be possible to view the status of the monitor point, that is, whether or not the input is active or inactive, through this "monitor and control" means.
    b. Any changes made to monitor point settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database are downloaded to that controller with the original hardware configuration settings.
    c. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

35. Monitoring and Controlling – Monitor Point Groups

    a. The software shall allow users to send commands to a monitor point group consisting of monitor points and doors (on one controller) through a system "monitor and control" means. These commands shall consist of setting or clearing the mask for all monitor points and door position inputs in the group. Setting a mask suppresses alarm conditions when the inputs are active, and clearing the mask restores the "visibility" of the alarms in the system. It shall also be possible to send other commands to arm or disarm active or inactive points only if one or more points are active or inactive, respectively.
    b. The software shall allow users to view the status of the monitor point group, that is, whether or not any inputs are active, through this "monitor and control" means.
    c. Any changes made to monitor point and door settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.
    d. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

36. Monitoring and Controlling – Global Monitor Point Groups

    a. The software shall allow users to send commands to a global monitor point group consisting of monitor points (from any controller) in the system through a system "monitor and control" means. These commands shall consist of setting or clearing the mask for all monitor points in the group. Setting a mask suppresses alarm conditions when the inputs are active, and clearing the mask restores the "visibility"

of the alarms in the system. It shall also be possible to send other commands to arm or disarm active or inactive points only if one or more points are active or inactive, respectively.

b. Any changes made to monitor point and door settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

c. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

37. Monitoring and Controlling – Control Points\

a. The software shall allow users to send commands to a selected control point in the system through a system "monitor and control" means. These commands shall consist of turning the control point on (energizing a relay with normal function or de-energizing a relay with inverted function), turning it off (de-energizing a relay with normal function or energizing a relay with inverted function), pulsing the control point once, or pulsing the control point repeatedly, if the control point is not a relay on legacy hardware.

b. The software shall allow users to view the status of the control point, that is, whether or not the point is energized, through this "monitor and control" means.

c. Any changes made to control point settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

d. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

38. AS. Monitoring and Controlling – Global Control Point Groups

a. The software shall allow users to send commands to a global group of control points in the system "on the fly" through a system "monitor and control" means. These commands shall consist of turning on all control points (energizing the relays with normal function or de-energizing the relays with inverted function), turning them off (de-energizing the relays with normal function or energizing the relays with inverted function), pulsing all control points once, or pulsing all control points repeatedly, if the control point is not a relay on legacy hardware.

b. Any changes made to the settings for the control points in the global group using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

c. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point

names with small icons or as a detailed list of names and current statuses of the points. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

39. Monitoring and Controlling – Auto Photo Recall

    a. The system shall provide the means to view a cardholder photo when a card is presented at a reader in the system. This photo recall window shall have a default configuration as well as options to configure customized photo recall layouts, as outlined elsewhere in this specification.
    b. The user shall be able to enlarge any photo in the photo recall display by moving the mouse cursor over the photo in the layout.
    c. The system shall automatically display a red border around a photo to visually identify the photo as representing a card that was denied access at a reader configured for the photo recall display.
    d. The user shall be able to expand the photo recall display to view additional cardholder and card information as selected for the customized photo recall configuration. The user shall additionally have the option to open the specific cardholder record directly from the photo recall window.
    e. The software shall allow a user to display in the photo recall window the doors and time zones to which a cardholder has rights when that cardholder's card is presented at a reader.

40. Monitoring and Controlling – Procedures

    a. The software shall enable users to alter how procedures resulting from triggers are executed through a system "monitor and control" means. These means shall allow procedures to be aborted, executed or resumed. Aborting a procedure shall stop a procedure during a delay action (in other words, while it is delayed) and all subsequent actions after the delay. Executing a procedure shall cause all the actions in the procedure to occur. Resuming a procedure shall execute actions remaining in a procedure if the procedure is in a delay.
    b. Changes made to the system through triggers and procedures using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.
    c. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names with optional descriptions of the points. These global procedures shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

41. Monitoring and Controlling – Transactions

    a. The software shall provide a monitor-transactions window that reports all system events and activity, such as access-granted and access-denied transactions, alarm states, door activity, change-of-state information and the like. The transactions appearing in this window shall not only report system events, but their appearance

shall define the starting point of system triggers that initiate system actions via the triggers and procedures as defined in this specification.

b. Users shall be able to configure the monitor-transaction window to display all or selected columns of information and/or to otherwise filter the display of information in the window, as described below. This configuration shall be selectable by means of the user's login, and it shall be possible for any login to have its own configuration. Systems incapable of such configuration of the monitor-transaction window shall be deemed unacceptable.

c. The software shall allow users to define the number of rows of transactions to display in the window, as well as selecting whether the most recent transaction appears at the top or at the bottom of the list in the window.

d. The software shall allow users to define the transaction source(s) of the displayed transactions, for example, whether all transactions appear or only those from I/O boards, or only those relating to access areas, etc. Users shall also be able to exclude various types of transactions, for example, request-to-exits, from display in the monitor transactions window.

e. The software shall allow users to define the site(s), channel(s), and controller(s) whose transactions are to be displayed in the monitor-transactions window. This feature shall allow only user-specified information to be displayed in the window.

f. The software shall allow users to customize the color and text used to display each type of transaction in the system making the transactions more visually-identifiable and text- specific for the users monitoring the system.

42. Monitoring and Controlling – User Commands

a. Users shall be able to use keypads connected into the system for the purpose of sending commands to the controllers. These commands shall be one of the following types: "Cipher mode" commands (see elsewhere in this specification) that allow a cardholder number to be entered at the keypad User commands that trigger a specific action in the system

b. It shall be possible to send user commands as numeric codes entered through a card- reader keypad to the controllers to trigger procedures (as described in this specification) in the system. The numeric code shall be entered as part of a trigger for a trigger and procedure action. User commands shall be capable of ranging from 1 to 8 digits in length.

43. Monitoring and Controlling – Component Status

a. Windows for the individual controllers and boards in the monitor and control "module" of the software shall permit selection and display of configurations, capacities, firmware versions, online and offline status, status of these controllers and boards as well as their individual components, (such as relays on these boards or controllers.)

44. Reports

a. The software shall provide the user with the capability to configure, customize and generate reports of system transactions, hardware and access-setting configurations,

cardholders, etc. It shall be possible to output generated reports to a local or network printer or in any of the following ways (output file types in parentheses): Microsoft® Excel spreadsheets (.xls), Adobe® PDFs (.pdf), Microsoft® Word documents (.doc), Crystal Report files (.rpt), or Rich Text files (.rtf) open-able by most word processors. Users shall be able to export the generated report using an intuitive file name of their own devising. When the report is displayed on the screen, the generated report shall appear in a window with a toolbar that will allow the user to scroll to the next or a previous page, go directly to the first or last page, jump to a specific page of the report, search for user- specified text anywhere in the report, and zoom in or out on the report page. Systems unable to provide such print previewing capabilities shall be unacceptable.

b. Users shall be able to generate the following system reports:
   1) Cardholders Reports
   2) Cardholders – Access Rights Reports
   3) Transaction History Reports
   4) Alarm Acknowledgements Reports
   5) Access Groups Reports
   6) Sites Reports Channels Reports Controllers Reports I/O Boards Reports Inputs Reports Outputs Reports
   7) Monitor Points Reports
   8) Monitor Point Groups Reports Control Points Reports Readers Reports
   9) Readers – Access Rights Reports
   10) Doors Reports Elevators Reports Triggers and Procedures Access Areas Reports Time Zones Reports Holidays Reports
   11) Card Formats Reports
   12) Maps Reports
   13) Icons Reports
   14) Daylight Saving Time Reports
   15) Print Journal Reports
   16) Custom Reports

c. The Cardholders report shall offer two modes of presentation: a list view and a detail view. The list view shall present a user-configurable display of information, and such information can be selected from among any fields in the cardholder database. The Detail view shall present a predefined layout of specific information. Both report modes shall be capable of displaying cardholder record information for all cardholders or those meeting specific user-defined search criteria. The amount of information displayed in the report shall depend on the size of the page and the widths of the columns in the report as selected by the user.

d. The Reports feature used for cardholder reports shall allow users to define single- or compound-search, or filtering, criteria to apply to determine the names of cardholders that appear in either a list report or detailed report. These searches shall be based on any field in the cardholder database. It shall be possible to save search criteria for later use. It shall also be possible to sort the records in the report in ascending or descending order based on data appearing in one or more selected fields in the cardholder database, such as last name, department, school grade and the like.

e. The Reports feature used for system and hardware reports shall also allow users to

define single- or compound-search, or filtering, criteria to apply to determine which system components or settings appear in the report. These searches shall be based on the fields in the database relevant to the selected module report. It shall be possible with these reports as well to save search criteria for later use. Records in the report likewise shall be sortable in ascending or descending order based on data appearing in one or more selected fields in the system database.

f. There shall be a user-selectable option in the Reports window to prevent the database fields that do not contain data from appearing in the list of fields available for use as search criteria. This option shall be activated by default in the software, so unused fields do not appear as columns in the report. This feature allows a user to find the fields needed for the report criteria more quickly and easily. The user shall be free to deactivate this option and so allow all of the database fields to appear and be available for selection.

g. Users shall be able to include selected header information to appear at the tops of generated reports. Capability shall exist as well to include custom logos or other image files as part of the header information. All reports shall have default descriptive names; however, it shall be possible for users to change the name of the report as it appears in the report header "on the fly

45. Peripherals

a. The system shall allow the use of commercial, off-the-shelf printers for printing of system activity reports.

46. Mapping

a. The system shall support an unlimited number of graphic files used as maps.
b. The system shall support the following graphic-file types for use as maps: bitmap (.bmp), enhanced metafile (.emf), graphics-interchange format (.gif), JPEG (.jpg), portable network graphics (.png), TIFF (.tif) and Windows® metafile (.wmf).
c. It shall be possible to display maps at the same time that other system windows (transaction windows, alarm acknowledgement windows and the like) appear on the screen.
d. Icons on the map shall be dynamic, that is, they shall be capable of changing their appearance in response to changes in the state of the hardware that they represent.
e. It shall be possible for users to zoom in on and out from any map.
f. The system shall provide a default library of multiple icons representing access-control functions.
g. The system shall support the addition of multiple customized icons designed and devised in third-party software programs such as Microsoft® Paint and the like.
h. The system shall provide an easy drag-and-drop means to drag hardware icons from a system hardware configuration window onto any desired map to create a dynamic icon that represents and displays the state of the hardware component represented on the tree. As a result, users shall be able to monitor the system and also control the components via the dynamic icons. Software that does not incorporate such a simple means to create dynamic icons on a map shall be deemed unacceptable.
i. Maps in the software shall allow the system name of a hardware component to be displayed above or below the dynamic icon representing that particular component

on the map. It shall as well be possible not to display a name. Icons on maps shall be capable of being individually resized.

47. Online Manual

    a. Selectable from the main menu of the software shall be a printable portable document file containing detailed instructions and background on the setup and operation of the system hardware components and a context-sensitive Help manual.

B. Acceptable Manufacturers

1. Identicard PremiSys Pro. Software to be installed on PC workstation.
2. No Substitutions

2.8 12V POWER SUPPLY

A. Specifications

1.	AC Input:	120 VAC, +10%, -13%
2.	DC Output:	12 VDC
3.	Line Regulation:	+/- .05% for a 10% change
4.	Load Regulation:	+/- .05% for a 50% load change.
5.	Output Ripple:	3 mV +.05% of output voltage, peak-to-peak maximum.
6.	Transient Response:	<50 microseconds for 50% load change.
7.	Short Circuit Protection:	Automatic current limit/fold back
8.	Stability:	+/-.05% for 24 hours after warm-up.
9.	Efficiency:	55%

10. An individual homerun cable is required between each field device powered by the power supply. The output of the power supply is to feed a series of fuses rated for the intended load on each homerun cable.
11. Size power supply based on current draw of field devices powered.
12. Built-in charger for sealed lead acid or gel type batteries.
13. Includes battery leads.

B. Acceptable Manufacturers:

1. Altronix. Provide battery backup capable of 1 hour run time. Coordinate power requirements with door hardware supplier.

2.9 24V POWER SUPPLY

A. Specifications

1. UL Listed, UL1481, UL603, UL294
2. Input 115 VAC/60 Hz.
3. Class 2-rated output.
4. 24 VDC power limited selectable output.

5. Maximum charge current .7 amp.
6. Filtered and electronically regulated outputs.
7. Built-in charger for sealed lead acid or gel type batteries.
8. Includes battery leads.
9. Automatic switch over to stand-by battery when AC fails.
10. Zero voltage drop when switched over to battery backup.
11. An individual homerun cable is required between each field device powered by the power supply. The output of the power supply is to feed a series of fuses rated for the intended load on each homerun cable.
12. Size power supply based on current draw of field devices powered.
13. Provide battery backup capable of one hour run time.

B. Acceptable Manufacturers:

1. Altronix. Provide battery backup capable of 1 hour run time. Coordinate power requirements with door hardware supplier.

2.10 PROXIMITY CARD READERS

A. Specifications

1. Proximity technology
2. Single piece construction
3. 26 bit
4. Compact modular design
5. Weather and vandal resistance
6. Weigand compatible
7. Cable distance, 500 feet

B. Approved Manufacturer
1. Identicard Linear Flexpass
2. No Substitutions

2.11 REQUEST-TO-EXIT PIR

A. Specifications:

1. Wall, door frame, or ceiling mount
2. Dual relay outputs
3. Adjustable range
4. 24 VDC power
5. Provide Kantech T-Rex trim plate

B. Acceptable Manufacturers:

1. Bosch DS160i
2. Approved equal

2.12 DOOR RELEASE PUSH BUTTON

A. Specifications

1. Momentary push button
2. Dry contact
3. 3 amp contact rating
4. Screw terminal connections
5. 11 gauge stainless steel single gang plate

B. Acceptable Manufacturers

1. Dukane 9A1895. Engrave panel "Door X Lock Release". Insert door number in place of X.

2. Approved Equal

2.13 ACCESS CONTROL WORKSTATION

A. Specifications

1. Tower
2. Windows XP Professional (with Service Pack 2 or higher)
3. PC – Core 2 Duo
4. 1GHz processor
5. 4 MB L2 cache
6. 2 GB DDR2 SDRAM (800 MHz)
7. 250 GB 7.2K RPM SATA Hard drive
8. 48x32 combo CDRW/DVD
9. Mouse
10. Keyboard
11. 19" FP LCD Monitor
12. 1024 x 768 24-bit video card
13. 1 serial and 1 parallel and 4 USB 2.0 ports
14. GB Ethernet port

B. Acceptable Manufacturer
1. Identicard
2. No Substitutions

2.14 SPEAKERS

A. Specifications

1. 2 watts total continuous power
2. 1 watt per channel @ 4 ohms
3. 2" x 3" full range driver
4. Power on/off and master volume control
5. Shielded

B. Acceptable Manufacturer

1. Altec Lansing Model 120
2. JBL
3. Audio Technica

2.15 OVERHEAD DOOR POSITION SWITCH

A. Specifications

1. 3' stainless steel armored cable
2. SPDT contacts
3. Wide gap read distance
4. Heavy cast aluminum housing
5. Floor-mounted

B. Acceptable Manufacturer:

1. Sentrol 2200 Series
2. Approved Equal

2.16 RECESSED DOOR POSITION SWITCH

A. Specifications:

1. 1- inch press-fit mounting
2. SPDT contacts
3. Heavy duty crush resistant mahogany color housing
4. Wide gap read distance

B. Acceptable Manufacturer:

1. UTC Fire & Security 1076W-M
2. Approved Equal

2.17 LOCAL ALARM SOUNDER

A. Specifications

1. 12-24 VDC
2. Current 0.010-0.018A
3. Contractor shall interface the sounding device to the access control system to audibly annunciate an intrusion alarm. The sounder shall be reset by the designated intrusion detection card reader.

B. Acceptable Manufacturers

1. Edwards Signaling E102A

2. Approved Equal

PART 3 - EXECUTION

3.1 INSTALLATION

A. All system programming shall be done at the contractor's facility prior to installation on site.

B. Qualified personnel shall install the System in strict compliance with manufacturer's instructions.

C. Wiring shall be color coded, uniform and in accordance with national electric codes and manufacturer's instructions.

D. Equipment shall be firmly secured, plumb and level.

E. All cable runs to the main equipment rack shall be tagged and identified.

F. Coordinate all work with other trades and Contractors.

G. Grounding of cables and peripheral equipment shall be installed per manufacturer's direction to eliminate noise induction and achieve optimum system performance.

H. Install and configure Security local area network as required for control and communication between system devices. When required, provide necessary coordination, termination, and programming associated with integrating Security local area network with facility network.

I. Equipment cabinets shall be assembled in the Contractor's shop prior to delivery to the job site.

3.2 SYSTEM OPERATIONAL SUPPORT

A. As part of the shop drawing submittal, the Contractor is required to submit a written report outlining the project specific functions and operational procedures of the access control system. This report will include the following-

1. The Contractor shall present proposed operational procedures for every function specified in Contract Documents or recognized as industry standard or convention for an access control system. All operational procedure possibilities will be presented to the Owner/User & Architect by the Contractor.
2. The Contractor shall address integration of the components and subsystems making up the control system when presenting the proposed operational procedures.
3. As a minimum the report shall contain the following:

    a. A procedural description of each and every control function.
    b. A procedural description of all administrative functions available to supervisory and maintenance personnel (e.g. log in code maintenance, alarm time zone programming).
    c. A preliminary technical description of how each function will be accomplished.
    d. Schedules of integrated actions (e.g.Duress alarms, auto dial to central station, etc.).

3.3 SOFTWARE SUPPORT

A. Prior to programming of the system, the Contractor shall request, in writing, scheduling of a system programming coordination meeting. This meeting is to take place during the product procurement, after submittals have been approved. A proposed agenda shall be included with the request.

B. The purpose of the coordination meeting is to define the project specific functions and operational procedures of the control system with the Owner/User and Architect.

C. The Contractor shall present proposed operational procedures for every function specified in Contract Documents or recognized as industry standard or convention. The Contractor will present all operational procedure possibilities to the Owner/User & Architect.

D. The Contractor shall address integration of the components and subsystems making up the control system when presenting the proposed operational procedures.

E. The Contractor shall prepare and present full size (for each GUI) drawings at this meeting. These drawings shall depict all screens with all information to scale. As a minimum, these screen drawings shall depict the following:

1. Overall building layout screen.
2. Location of all controlled doors and alarm points.
3. Floor control screens. (These area screens should be drawn to represent actual orientation with control officer's view).
4. All special control and transition screens.
5. Each sheet should be numbered for easy reference.
6. Screens should be printed in color.

F. The contractor shall refrain from any programming of the Access Control system until after the Architect has reviewed and approved the programming report.

G. The Owner/User and Architect reserve the right to change programming of the Access Control System after installation and prior to final acceptance.

H. The contractor shall assist the Owner/User in developing a badge template. This will include importing of digital photos, custom graphics, and text.

3.4 SYSTEM INITIALIZING AND PROGRAMMING

A. All programming shall occur in the Contractor's shop prior to installation on site.

B. The System shall be turned on and adjustment made to meet requirements of the specification and on-site conditions.

C. The System shall be programmed to function as specified.

D. Any special programming shall be documented and a written copy given to the Owner/User.

E. Coordinate integration of other electronic systems as called for in the contract documents.

3.5 SYSTEM TEST PROCEDURES

A. The System shall be completely tested to assure that all components are hooked up and in working order. Inspect system for defects. Correct all causes of such defects. If the cause is outside of the scope of the Division 28 series scope of work, promptly notify the Architect is writing, indicating the cause of the defect and suggested corrective procedures.

B. The contractor is to verify the system is communicating with all controlled devices.

C. Test 120VAC power equipment and hardware internal to all equipment racks. Test all conductors for shorts, opens, and polarity.

D. Verify operation of battery backup. Test by removing power from system.

E. Verify all field wiring is free of shorts and opens prior to termination of head end electronics.

F. After termination of head end electronics, full test operation of system including activation of field devices, alarm initiation from field devices, tone alert as activated by alarms, and central station dialing.

G. Provide written documentation showing all test results.

H. The System shall be final tested in the presence of the Architect. Contractor is to provide all required testing equipment.

3.6 TRAINING

A. Contractor is responsible for providing operational and maintenance training applicable to the entire control system. Training is to include, but not be limited to the following-

1. Review all O+M manuals with Owner/Users representatives present for training.
2. Perform a tour of the entire facility. During the tour the trainer shall point out all control equipment and provide a brief description of its purpose and use. This is to include but not be limited to control panels (graphic and pushbutton), all control system hardware, and devices controlled.

3. Explain functionality and operation of controlled entrances including-
   a. Overhead doors
   b. Architectural doors

3.7 INSTRUCTION SET 1: COM. RM. 129

A. Provide all control panels, remote input/output boards, network converters, access control power supplies in room 129 as noted on the floor plans. All low voltage power supplies will be mounted on the walls.

3.8 INSTRUCTION SET 2: DOOR 121A

A. Theory of operation: Door will be secured with electric latch retraction. Entry will be obtained with a valid card read on the card reader. Program door to generate an alarm that will notify

personnel if breached.

B. Provide one Belden access control cable bundle from the door location to Comm. Rm.129 head end equipment location.
C. Provide one card reader, one ELR device on the active leaf, one door position switch on each leaf, one power transfer hinge, one request to exit button, and one egress sensor.
D. Provide one local power supply within 50' of this opening. Provide 110VAC power at the local power supply.
E. Provide electrified locking hardware per reference detail
F. Provide junction boxes and conduit from device locations to nearest accessible location at ceiling.

3.9 INSTRUCTION SET 3: DOORS 101A, 105B

A. Theory of operation: Doors will be monitored for status by the access control system. Program door to generate an alarm that will notify personnel if breached.
B. Provide cabling from the door location to Comm. Rm. 129 head end equipment location.
C. Provide one door position switch on each leaf and one egress sensor.
D. Provide conduit from device location to nearest accessible location at ceiling.

3.10 INSTRUCTION SET 4: DOORS 113, 132, 140A, 140B

A. Theory of operation: Doors will be secured with electric strike with a card reader on both sides of the door.
B. Provide cabling from the door location to Room 129 head end equipment location.
C. Provide two card readers, one electric strike, and one door position switch at doors 113, 132, 139A.
D. Provide a local piezo alarm sounder at door 113, & 132 to be activated in the event that the room is exited without a valid card being presented to the reader.
E. Provide and install two card readers and one door position switch at doors 140A, & 140B. Electronic locking hardware for these doors will be detention grade and will be supplied by others.
F. Provide electrified locking hardware for doors 113, 132 are to be provided and installed by Security Contractor.
G. Provide conduit from device location to nearest accessible (drop tile) ceiling.

3.11 INSTRUCTION SET 5: DOORS 109A, 109B, 129, 151, 154, 161B

A. Theory of operation: Doors will be secured with an electric strike with access from outside the room using a card reader at all times.
B. Security Contractor will provide and cabling from the door location to Comm. Rm. 129 head end equipment location.
C. Security Contractor will provide and install one card reader, one electric release (L6514), one door position switch, and one egress sensor at each door.
D. Security Contractor will provide a latch protector at doors 151 and 154.
E. Electrical contractor will provide conduit from device location to nearest accessible (drop tile) ceiling.
F. Door hardware provider to provide a storeroom function lockset for each door.

3.12 Instruction Set 6: Door 114

A. Theory of operation: Door will be secured with electrified trim. An electric transfer hinge will be provided and the inactive leaf of the door will be cored for routing the cable. A card reader will be used from the inside to open this door to allow transfer of evidence from vehicles into the evidence room. No exterior hardware will be on this door for a higher level of security.
B. Security Contractor will provide and install cabling from each door location to Comm. Rm.129 head end equipment location.
C. Security Contractor will provide and install a card reader, an electronic lock, and two door position switches on the door.
D. Electrical contractor will provide conduit from device location to nearest accessible (drop tile) ceiling.
E. All perimeter doors will be programmed to generate an alarm that will notify personnel.

3.13 Instruction Set 7: Doors 146A, 146B

A. Theory of operation: Doors will be secured with a card reader with access from secured side using a card reader at all times.
B. Security Contractor will provide and install cabling from each door location to Comm. Rm. 129 head end equipment location.
C. Security Contractor will provide and install one card reader and one overhead door position switch at each door. Doors 146A, & 146B will have their card readers and notification lights installed on a pedestal centrally located so that the vehicle can gain access to the appropriate bay. Also included on this pedestal will be lights that will indicate whether or not the bay is in use. Doors 146B will have their card readers located on the wall next to them to allow egress from the sally port.
D. Security Contractor will provide and install a vehicle loop detector in each of the two bays in the sally port.
E. The existing overhead door operators will be integrated into the access control system to control the opening and closing of these overhead doors.
F. Each of these doors will be integrated with an interlock system.
G. Electrical contractor will provide conduit from device location to nearest accessible (drop tile) ceiling.

3.14 INSTRUCTION SET 7A/DOORS 161A

A. Theory of operation: Doors will be monitored for status using an overhead door position switch.
B. Security Contractor will provide and install one cabling from each door location to Comm. Rm. 129 head end equipment location.
C. Provide and install one overhead door position switch at each door.
D. Provide conduit from device location to nearest accessible (drop tile) ceiling.

3.15 INSTRUCTION SET 8: INTERLOCK BETWEEN 139B AND 140A

A. Theory of operation: Prevent the any of the doors from opening simultaneously.
B. Security Contractor to provide necessary equipment to provide an interlock between these three openings. This will prevent the three of these openings from being unlocked simultaneously.
C. Security Contractor to provide and install the interlock relay board and connects doors 139B and

140A.

3.16 INSTRUCTION SET 9/INTERLOCK BETWEEN 140A AND 140B

A. Theory of operation: Prevent the both doors from opening simultaneously.
B. Provide necessary equipment to provide an interlock between these two openings. This will prevent both of these openings from being unlocked simultaneously.
C. Provide and install the interlock relay board and connects doors 140A and 140B.

3.17 INSTRUCTION SET 10: INTERLOCK BETWEEN 140B, 146A, 146B

A. Theory of operation: Prevent the any of the overheads from opening when door 140B is open.
B. Provide necessary equipment to provide an interlock between these two openings. This will prevent both of these openings from being unlocked simultaneously.
C. Provide and install the interlock relay board and connect doors 140B, 146A, 146B.

3.18 INSTRUCTION SET 14: LCD DISPLAY, NOTIFICATION LIGHT AND ARM/DISARM READER RECEPTION AREA & DEPUTY WORK ROOM

A. Theory of operation: An LCD display and card reader will be installed both in room 110. The card reader will be used to arm and disarm the intrusion detection system and the LCD display will be used to monitor the status of the system. Using card readers for arming and disarming follows the Loudoun County standard of operations and provides a higher level of security than using alarm codes to arm and disarm the systems.
B. Security Contractor will provide and install cabling from each location to Comm. Rm. 129.

C. Security Contractor will provide and install one LCD display, one alarm notification light, and one card reader at each location.
D. The card reader will allow users to arm and disarm their partition using an access card in lieu of codes. The notification light will activate when duress is activated and the LCD display is to show which duress button was activated as well as show the status of the alarm system.
E. Electrical contractor to provide conduit from each location to nearest accessible (drop tile) ceiling.

3.19 INSTRUCTION SET 15: KEYSWITCH OVERRIDE, REMOTE RELEASE BUTTON

A. Theory of operation: A Keyswitch override button and remote release button will be installed in the Reception room. The remote release will allow staff to unlock the door 122B that leads into corridor 146. Loudoun County buildings are equipped with a Keyswitch override which will allow personnel to secure the building outside the automatic locking/unlocking schedule. All exterior doors that follow auto scheduling will be included in this Keyswitch override to ensure the building is secure when override is in engaged.
B. Security Contractor will provide and install cabling from each location to Comm. Rm. 129.
C. Security Contractor will provide and install one Keyswitch override and one remote release button at each location. Exact device location is to be coordinated with Architect and Owner.
D. Electrical contractor to provide conduit from each location to nearest accessible (drop tile) ceiling.

3.20 INSTRUCTION SET 16: EVIDENCE ROOM – 132/DOOR 132

A. Theory of operation: Door will be secured with an electric strike with access from both sides using a card reader at all times. An arm/disarm reader and LCD display will also be installed at this location to arm and disarm the evidence room alarm system. Two motion detectors will be installed to monitor the space for unauthorized access
B. Furnish and install cabling from door location to Comm. Rm.129 head end equipment location.
C. Security Contractor will provide and install two card readers, one arm/disarm card reader, one LCD display, one electric release, and two door position switches at the door. Two motion detectors will also be installed inside the room.
D. Electrical contractor will provide conduit from device location to nearest accessible (drop tile) ceiling. Coordinate final turn-out location with Security Contractor
E. Door hardware provider will provide a lockset with a rigid handle on both sides.

3.21 INSTRUCTION SET 17: DURESS BUTTONS (140, 110)

A. Theory of operation: A duress button will be installed at the designated location. This duress button will cause a local alarm as indicated on drawings and can also be programmed to dial out to the ECC.
B. Security Contractor will install a duress button at each location, final location to be coordinated with Architect and Owner.
C. Security Contractor will integrate duress button into local notification devices located in the Deputy Work Room (123) and Reception (110).
D. Loudoun County will provide connection to ECC if required.

3.22 INSTRUCTION SET 18: VEHICLE GATES

A. Theory of operation: There are five vehicle/man gates that will be controlled using card readers to gain entry. The card readers will be installed on a pedestal. All required conduit from the pedestal location will be provided back into the main building and all automatic gate operators, loops, and loop detectors will be provided by others.
B. Security Contractor will install a pedestal, card reader, and intercom at each designated location as coordinated with Architect and Owner.
C. Security Contractor will integrate the card readers with the gate operators to provide proper operation.
D. Electrical Contractor will provide conduit to each pedestal location back to the main building. Size and locations to be coordinated with Security Contractor.
E. Gate provider to provide all automatic operator, loop detectors, inputs, outputs, and exit and safety loops as required ensuring proper integration with the access control system.

END OF SECTION 281300